

Serial No. 09/503,205

IN THE CLAIMS:

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

Please AMEND claims 1 and 8 in accordance with the following:

1. (CURRENTLY AMENDED) A data generating apparatus, comprising:
an input device inputting a condition specified by a user for designating a finite field corresponding to a mathematical finite aggregate in which four arithmetical operations are defined, a number of elements of the finite aggregate being expressed as p^m with p and m as a prime number and a positive integer indicating an extension degree, respectively;
a generation device automatically generating expression data of the finite field based on the inputted condition; and
an expression data storage device storing the generated expression data.
2. (ORIGINAL) The data generating apparatus according to claim 1, further comprising an operation device performing a finite field operation based on the expression data stored in said expression data storage device.
3. (PREVIOUSLY PRESENTED) The data generating apparatus according to claim 1, wherein when a bit length of the prime number is inputted as the condition, said generation device automatically generates prime number data corresponding to the bit length and stores the generated prime number data in said expression data storage device.
4. (PREVIOUSLY PRESENTED) The data generating apparatus according to claim 1, wherein when the extension degree is inputted as the condition, said generation device automatically generates irreducible polynomial data corresponding to the extension degree and stores the irreducible polynomial data in said expression data storage device.
5. (ORIGINAL) The data generating apparatus according to claim 4, wherein when an instruction using an optimal normal basis is inputted, said generation device automatically generates irreducible polynomial data for an optimal normal basis corresponding to the extension

Serial No. 09/503,205

degree and the irreducible polynomial data for an optimal normal basis in said expression data storage device.

6. (ORIGINAL) The data generating apparatus according to claim 1, further comprising a fixed data storage device storing one or more pieces of predetermined expression data of a finite field,

said generation device stores expression data of a finite field corresponding to the condition in said expression data storage device if there is the expression data of a finite field corresponding to the condition in the fixed data storage device, and said generation device automatically generates expression data of a finite field corresponding to the condition if there is no expression data of a finite field corresponding to the condition in the fixed data storage device.

7. (PREVIOUSLY PRESENTED) The data generating apparatus according to claim 1, further comprising:

a designation device designating expression data of a finite field; and

a verifier device verifying whether the designated expression data are suitable, the verifier device storing designated expression data in said expression data storage device if the designated expression data are suitable, and the verifier device asks the designation device for other expression data if the designated expression data are not suitable.

8. (CURRENTLY AMENDED) A computer-readable storage medium on which is recorded a program enabling a computer to execute a process, said process comprising:

specifying a condition;

automatically generating expression data of a finite field corresponding to a mathematical finite aggregate in which four arithmetical operations are defined, a number of elements of the finite aggregate being expressed as p^m with p and m as a prime number and a positive integer indicating an extension degree, respectively; and

outputting the generated expression data.

9. (PREVIOUSLY PRESENTED) A data generating method, comprising:

designating a condition for designating a finite field corresponding to a mathematical finite aggregate in which four arithmetical operations are defined, a number of elements of the finite aggregate being expressed as p^m with p and m as a prime number and a positive integer indicating an extension degree, respectively;

Serial No. 09/503,205

automatically generating expression data of the finite field based on the designated condition; and

supplying the generated expression data to a finite field operation apparatus.

10. (PREVIOUSLY PRESENTED) A data generating apparatus, comprising:

inputting means for inputting a condition for designating a finite field corresponding to a mathematical finite aggregate in which four arithmetical operations are defined, a number of elements of the finite aggregate being expressed as p^m with p and m as a prime number and a positive integer indicating an extension degree, respectively;

generating means for automatically generating expression data of the finite field based on the inputted condition; and

expression data storing means for storing the generated expression data.

11. (PREVIOUSLY PRESENTED) A data generating apparatus, comprising:

an input device inputting a condition designating a finite field; and

an expression data storage device storing expression data of the finite field,

wherein the expression data is based on the inputted condition.

12. (PREVIOUSLY PRESENTED) The data generating apparatus according to claim

11, further comprising an operation device performing a finite field operation based on the stored expression data.

13. (PREVIOUSLY PRESENTED) The data generating apparatus according to claim

11, further comprising a generation device automatically generating the expression data of the finite field.

14. (PREVIOUSLY PRESENTED) The data generating apparatus according to claim

13, the generation device generates at least one of prime number data corresponding to a bit length of the finite field and irreducible polynomial data corresponding to an extension degree that describes the finite field, and stores the generated data in the expression data storage device.

15. (PREVIOUSLY PRESENTED) The data generating apparatus according to claim

11, further comprising:

a designator designating the expression data of the finite field; and

Serial No. 09/503,205

a verifier verifying whether the designated expression data is suitable, storing the suitable designated expression data in the expression data storage device, and requesting other expression data from the designator if the designated expression data are not suitable.

16. (PREVIOUSLY PRESENTED) A data generating method, comprising:
designating a condition for a finite field;
generating designated expression data of the finite field based on the designated condition; and
storing the generated designated expression data.

17. (PREVIOUSLY PRESENTED) The data generating method according to claim 16, further comprising
performing a finite field operation based on the stored designated expression data.

18. (PREVIOUSLY PRESENTED) The data generating method according to claim 16, wherein the generating designated expression data comprises generating at least one of prime number data corresponding to a bit length of the finite field and irreducible polynomial data corresponding to an extension degree that describes the finite field.

19. (PREVIOUSLY PRESENTED) The data generating method according to claim 16, further comprising
verifying whether the generated designated expression data is suitable; and
generating other expression data if the designated expression data are not suitable.